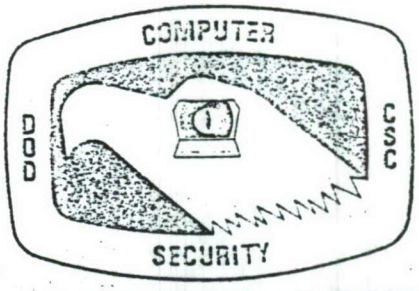
FINAL EVALUATION REPORT RESOURCE ASSESS CONTROL

(U.S.) Department of Defense
Ft. Mead, MD

Jul 84

U.S. DEPARTMENT OF COMMERCE
National Technical Information Service
NTIS®

CSC-EPL-84/001



FINAL EVALUATION REPORT

Resource Access Control Facility (RACF)

Version 1 Release 5

23 JULY 1984

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS AD-A150625
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for Public release; Distribution unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) CSC-EPL-84/001	5. MONITORING ORGANIZATION REPORT NUMBER(S) S-225,284
6a. NAME OF PERFORMING ORGANIZATION Department of Defense Computer Security Center 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State and ZIP Code) 9800 Savage Road Ft. Meade, MD 20755-6000	7b. ADDRESS (City, State and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State and ZIP Code)	10. SOURCE OF FUNDING NOS. PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT NO.
11. TITLE (Include Security Classification) ~~DRAFT~~ Resource Access Control Facility Version 1 Release 5 Final Evaluation Report	
12. PERSONAL AUTHOR(S) *MITRE CORP. ISRAEL, Howard; LAFOUNTAIN, Steven; MONSEIN, Johnathan; CHEN, Thomas*; JORDAN, Robert*	
13a. TYPE OF REPORT Final 13b. TIME COVERED FROM _____ TO _____	14. DATE OF REPORT (Yr., Mo., Day) 84/07/23 15. PAGE COUNT
16. SUPPLEMENTARY NOTATION	

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB. GR.	Trusted Computer System Evaluation Criteria, Resource Access Control Facility, C1, EPL, DoDCSC, RACF, IBM, MVS

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The security features of RACF/MVS were evaluated against the requirements specified by the DoD Trusted Computer System Evaluation Criteria dated 15 Aug 83 and found to satisfy all the requirements of evaluation Class C1.

The Department of Defense Computer Security Center (DoDCSC) was established in January 1981 to encourage the widespread availability of trusted computer systems for use by facilities processing classified or other sensitive data.

In the first quarter of FY83, International Business Machines Inc., (IBM), requested that the DoDCSC evaluate their commercially available Resource Access Control Facility (RACF) Program Product Version 1, Release 5 for the OS/VS2 MVS operating systems as specified in the RACF General Information Manual. MVS is an IBM operating system for its 303x, 308x, 4341, 370/158, and 370/168 processors.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☒ DTIC USERS ☐	21. ABSTRACT SECURITY CLASSIFICATION Unclassified
22a. NAME OF RESPONSIBLE INDIVIDUAL Mario Tinto	22b. TELEPHONE NUMBER (Include Area Code) 301-859-6044 22c. OFFICE SYMBOL C12

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE.

SECURITY CLASSIFICATION OF THIS PAGE

N O T I C E

THIS DOCUMENT HAS BEEN REPRODUCED FROM THE BEST COPY FURNISHED US BY THE SPONSORING AGENCY. ALTHOUGH IT IS RECOGNIZED THAT CERTAIN PORTIONS ARE ILLEGIBLE, IT IS BEING RELEASED IN THE INTEREST OF MAKING AVAILABLE AS MUCH INFORMATION AS POSSIBLE.

FOREWORD

This publication, ~~IBM~~ Resource Access Control Facility (RACF) Version 1 Release 5 Final Evaluation Report, is being issued by the DoD Computer Security Center under the authority and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this report is to document the results of the formal evaluation of IBM's RACF security package. The requirements stated in this report are taken from the Department of Defense Trusted Computer System Evaluation Criteria dated 15 August 1983.

Approved:

Robert L. Brotzman

Robert L. Brotzman
Director
DoD Computer Security Center

23 July 1984

Table of Contents

EVALUATION TEAM MEMBERS

Howard M. Israel
Steven M. La Fountain
Jonathan R. Monsein
DoD Computer Security Center
9800 Savage Road
Fort George G. Meade, MD 20755-6000

Thomas M. Chen
Robert T. Jordan
The MITRE Corporation
P. O. Box 208
Bedford, MA 01730

EXECUTIVE SUMMARY

The security protection provided by the IBM Resource Access Control Facility (RACF) Version 1, Release 5 running with the Multiple Virtual Storage/System Product (MVS/SP) 1.3.2 operating system has been evaluated by the Department of Defense Computer Security Center (DoDCSC). The security features of RACF/MVS were evaluated against the requirements specified by the Trusted Computer System Evaluation Criteria (the Criteria) dated 15 August 1983.

The DoDCSC evaluation team has determined that the highest class at which RACF/MVS satisfies all the specified requirements of the Criteria is class C1 and therefore RACF/MVS has been assigned a class C1 rating.

Further, RACF/MVS was found to satisfy all requirements of class C2 **except** for the Object Reuse requirement. It appears, however, that this problem can be corrected. There exists a documented set of modifications for MVS Release 3.8 that cause all disk space to be erased before becoming eligible for reuse. These modifications however, were not present in the system used for the functional testing of this evaluation and have not been evaluated.

A system that has been rated as being a C division system contains the features and assurances described in the Criteria. There is no assurance that a C division system is free of flaws that would allow the subversion or bypassing of the advertised security mechanisms through penetration methods.

At the time of the evaluation MVS was the only operating system that supported RACF Version 1 Release 5. The integrity of RACF is dependent upon the integrity of the MVS system itself.

SECTION 1

INTRODUCTION

1.1 BACKGROUND

The Department of Defense Computer Security Center (DoDCSC) was established in January 1981 to encourage the widespread availability of trusted computer systems for use by facilities processing classified or other sensitive data.

In the first quarter of FY 83, International Business Machines Corp. (IBM) requested that the DoDCSC evaluate their commercially available Resource Access Control Facility (RACF) Program Product Version 1, Release 5 for the OS/VS2 MVS operating systems as specified in the RACF General Information Manual. MVS is an IBM operating system for its 303x, 308x, 4341-2, 4341-11, 370/158, and 370/168 processors.

1.2 EVALUATION PROCESS

The DoDCSC established an evaluation team, and the evaluation process commenced with a meeting on 1 November 1982 at IBM's Washington Systems Center in Gaithersburg, MD. At this meeting IBM and the DoDCSC committed themselves to complete a formal evaluation of RACF/MVS. The DoDCSC evaluation team would examine and evaluate the security features of RACF/MVS against the final draft of the Trusted Computer System Evaluation Criteria that was to be issued in January of 1983 (the evaluation was later updated to use the 15 August version of the Criteria). Following the completion of the evaluation, the team would issue a report that detailed the evaluation. RACF/MVS would then be assigned a rating and be placed on the DoDCSC's Evaluated Products List (EPL).

The evaluation team began their examination of RACF/MVS by attending MVS classes and RACF demonstrations, reviewing RACF documentation, and gaining hands-on experience with RACF at a training session held at IBM/Gaithersburg in December 1982.

The evaluation team met with IBM on 26 January 1983 at the IBM facility in Poughkeepsie, NY to discuss the progress of the evaluation and to attend IBM presentations describing MVS integrity and IBM product assurance and testing.

A detailed test plan was developed and sent to IBM for review. The evaluation team then met with IBM personnel in March at the IBM facility in Wappinger Falls, NY to discuss the test plan and to examine and review documentation of IBM's own internal testing of Version 1 Release 5 of RACF.

The security features functional testing was conducted at the IBM Washington Systems Center on 5-7 April 1983. This testing was conducted on a 3081 Model K running MVS/SP 1.3.2 with 32 Megabytes of real storage, Job Entry Subsystem 2 (JES2) (maintenance level 8301), RACF Version 1 Release 5, Time Sharing Option/Extended (TSO/E), Session Manager, and Interactive System Productivity Facility (ISPF). After completing the functional testing, there is no penetration testing (i.e., subversion of the system) required for a C division evaluation, and an analysis of the test results, the evaluation team prepared this final report.

1.3 EVALUATION ENVIRONMENT

RACF is IBM's MVS facility (at the time of the evaluation RACF Version 1 Release 5 did not run on any other operating system) that provides controlled access to system resources. RACF utilizes the Standard MVS Security Interface. This interface causes MVS to call for RACF authorization checking at every LOGON, OPEN, ALLOCATE, SCRATCH, and RENAME. Numerous RACF options, selectable at installation time, provide a high level of discretionary security. The owner of a resource is allowed to specify and control access to that resource. This access can be given in various degrees (ALTER, CONTROL, UPDATE, READ, and NONE).

ALTER - for discrete profiles, allows control over the resource and the ability to authorize other users access to that resource.

- for generic profiles, ALTER allows control over the resource but only the owner of the resource has the ability to grant access to other users.

CONTROL - applies only to Virtual Storage Access Method (VSAM) data sets and allows the specified user to retrieve, update, insert, and delete records in that data set.

UPDATE - allows for reading and writing.

READ - allows a user access for the purpose of reading only.

NONE - prohibits the specified user from gaining any type of access to the specified resource.

RACF also protects access to the system itself. RACF requires that each user who is defined to RACF supply a unique userid and password before being allowed access to the system (NOTE: RACF does allow undefined users to exist on the system but limits their accesses to only unprotected resources (i.e., resources that are not defined to RACF) and to the specified Universal Access (UACC) level of any RACF-protected resource). A

user who submits a batch job to the system without supplying a userid and password is treated as undefined by RACF and access will be limited to the UACC level of any protected resource.

The installation has the ability to define syntax rules with which all passwords must comply. These rules govern the length and the alphanumeric syntax of the password. The installation may also define a maximum time interval within which the user must change his password and a maximum number of consecutive times that a user can supply an invalid password before his userid is revoked. When a userid is revoked by RACF, the userid must be reset by the security administrator before that userid is again allowed to access the system.

RACF can provide protection by default (when the proper options are set by the installation). A "default" access rule capability is available with profile modeling. Profile modeling can be used to implement "default" protection by defining a model profile for each user and/or group. This model profile can contain the UACC level, auditing flags, owner, level, installation-defined data, and access lists. Further, the SETROPTS command can be used to turn on RACF resource checking for resource classes defined to RACF, so that all accesses to that resource class are checked by RACF.

Default protection of data sets may be imposed selectively, by data set name qualifier, for as many or few existing or still-to-be-created data sets as the installation chooses. Additionally, newly created Direct Access Storage Device (DASD) data sets receive automatic protection by default when the Automatic Data Set Protection (ADSP) attribute is specified for the creator. It should be noted that a user who possesses the OPERATIONS attribute may still access any data set created under ADSP unless he is specifically denied access by a resource profile.

RACF also provides extensive audit capabilities by writing to the MVS System Management Facility (SMF) data sets. The default is to write a record into SMF whenever a detected, unauthorized access attempt is made. There is also the ability to log authorized accesses. This is done by specifying the appropriate entry in the access rules.

The RACF Report Writer is a versatile and useful tool. The Report Writer can be used to obtain reports on detected unauthorized access attempts, successful authorized accesses, or on a user and/or resource basis. The Report Writer can also be used to generate a single report containing all of this information.

For the maximum security possible, RACF should be implemented to supply default protection of <u>all</u> resources in the

system, all users of the system should be defined to RACF and given the minimum amount of authority that will allow them to efficiently and effectively use the system. Passwords should be enforced and regular password change should be implemented. Finally, the RACF audit facilities should be used to the maximum, reasonable extent and the Report Writer should be regularly used to obtain information about which users are utilizing what resources and how.

1.4 DOCUMENT ORGANIZATION

This report consists of six major sections. Section 2 provides the class C1 requirements, as stated in the Criteria, and describes the security features and the testing that resulted in RACF/MVS being assigned a class C1 rating. Section 3 compares the features of RACF/MVS with the class C2 requirements that were **not met by RACF**, describes the testing, and details the reasons why RACF/MVS did not achieve a class C2 rating. Section 4 describes RACF/MVS features that exceed the requirements of class C1 as well as the evaluation of those features. Section 5 presents comments by the evaluation team concerning specific RACF/MVS features and a recommended mode of implementing RACF. Section 6 presents the conclusions of this report. The appendix provides a detailed description of the testing conducted for the evaluation.

SECTION 2

RACF VS. CLASS C1 REQUIREMENTS

THIS SECTION ADDRESSES THE CLASS FOR WHICH RACF SATISFIES ALL REQUIREMENTS OF THE CRITERIA.

2.1 DISCRETIONARY ACCESS CONTROL

Requirement:

The Trusted Computing Base (TCB) shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals or defined groups or both.

Satisfied By:

Discretionary access control information is contained in the RACF profile data set which defines who (userid) has access to what (resources) and how (access rights can be set to ALTER, CONTROL, UPDATE, READ and/or NONE). Controlled sharing is specified by defining user profiles which contain information about the user's identity, responsibilities, names of the groups to which he is connected, and other miscellaneous data used by RACF. Users can be placed in logical groups, and each user in a group can be granted different access rights.

Although RACF normally protects only those resources that are defined to it, RACF can provide protection by default (when the proper options are set by the installation). A "default" access rule capability is available with profile modeling. Profile modeling can be used to implement "default" protection by defining a model profile for each user and/or group. This model profile can contain the universal access authority, auditing flags, owner, level, installation-defined data, and access lists. Testing verified that model profiles can be created on a user or group basis to contain the default access parameters for the newly created data set. Further, the SETROPTS command can be used to turn on RACF resource checking for resource classes defined to RACF, so that all accesses to that resource class are checked by RACF.

Other defaults are supplied with individual RACF commands, e.g., the AUDIT option for a Direct Access Storage Device (DASD) data set defaults to the audit of access failures. Further, installation exits can be programmed for an always-call situation

in which different implementations can be tailored for the exact needs of the installation.

Testing verified that default protection can also be implemented through the use of the Generic Profile facility. Default protection of data sets may be imposed selectively, by data set name qualifier, for as many or few existing or still-to-be-created data sets as the installation chooses. Additionally, newly created DASD data sets receive automatic protection by default when the Automatic Data Set Protection (ADSP) attribute is specified for the creator, and/or by the existence of the appropriate generic profile. Further, default access rule capability is available with profile modeling, which copies the access rules for each new data set from a user's or group's model. It should be noted that a user who possesses the OPERATIONS attribute, may still access any data set created under ADSP unless he is specifically denied access by a resource profile.

During the evaluation, attempts were made to circumvent discretionary protection by exploiting the Global Access Checking (GAC) facility. The GAC facility provides a means of avoiding the overhead of checking the RACF profiles for frequently accessed resources. The GAC facility consists of a table of permitted accesses to selected resources. Access attempts first encounter the GAC prior to the checking of the RACF profiles. If the access is permitted by the GAC facility, the remainder of the RACF checking and auditing is bypassed. The GAC can grant but never deny access. If the requested access is not in the GAC table, RACF proceeds to check the RACF profiles for authorization.

The attempts to exploit the GAC facility involved submitting commands by unauthorized users to add entries to the GAC table. All attempts to create GAC table entries by a user without the SPECIAL attribute failed.

2.2 IDENTIFICATION AND AUTHENTICATION

Requirement:

The Trusted Computing Base (TCB) shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user.

Satisfied By:

RACF determines if a user possesses the necessary authority to access a RACF protected resource for the operation to be performed. Users are identified by a unique userid and their identity is verified by password and/or operator identification card supplied during logon.

RACF requires that each user attempting to access any RACF protected resource in the system be defined to RACF through a unique userid. If a user is not defined to RACF, all his access attempts (except when universal access (UACC) has been specified as some value other than NONE) to RACF protected resources are denied.

A user is defined to RACF via the RACF ADDUSER command. The user controls his password and can change it himself. The user's identity is verified by the system, at Time Sharing Option (TSO) logon, batch job initiation, Information Management System (IMS) and Customer Information Control System (CICS) sign-on and Network Communication Control Facility (NCCF) operator sign-on.

RACF enforces password change. During the testing, password expiration dates and syntax rules were set so that users had to change their passwords accordingly. When a password expires, a warning message is issued at login time. RACF has the ability to retain up to 32 previous passwords for each user so that passwords can not be repeated. The password syntax rules, which are set by the installation, specify the length and alphanumeric structure of new passwords. If a new password does not satisfy the installation defined syntax rules, the password is not accepted and the old password remains in effect, unless it has expired, in which case a syntactically correct new password must be entered for a successful login.

Passwords are stored in a scrambled form within the RACF data set. The algorithm used for this scrambling is the same for all RACF installations. This data set contains all RACF access control information and therefore should be protected by RACF. If a resource is password protected by MVS as well as by RACF, the MVS password will be ignored.

RACF provides an option to let the installation determine the number of consecutive times that a user can enter an invalid password, after which the userid is automatically revoked until reset by the security administrator. The number of invalid password attempts is variable up to 255. Messages concerning unsuccessful attempts to enter the system immediately appear on the security console (and any other console defined with a message route code of 9).

TSO passwords are not echoed back to the terminal screen.

At no time during the test period were there any indications of TSO password exposure. However, as a caution, physical security should be enforced in order to prevent password exposure from batch Job Control Language (JCL) files. JCL card decks contain the password on the job cards, making physical card decks a potential exposure. Note that when a user is processing a batch job, or editing a batch stream file, passwords may be displayed on the screen unless these passwords are suppressed by inputting a series of question marks in the place of the passwords in the file.

It should be noted that users can be defined to the system without being defined to RACF. Such users are able to log on to the system without supplying a RACF password (although an MVS password may be required) and can only access resources not protected by RACF or RACF protected resources for which a UACC value other than NONE has been specified.

2.3 SYSTEM ARCHITECTURE

Requirement:

The Trusted Computing Base (TCB) shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system.

Satisfied By:

RACF can be and should be set to protect all of its own data sets, routines, functions, etc. Within the RACF/MVS system software environment there is an identifiable Trusted Computing Base composed of MVS, RACF, Job Entry Subsystem (JES2 or JES3) and the necessary system utilities and access methods.

In addition to RACF's security features, the following are relevant MVS/SP protection mechanisms. MVS implements two techniques to preserve the integrity of each user's work. The first is a private address space for each user and the second is the use of multiple storage protect keys.

In MVS, a virtual storage address space consists of a system area, a common area, and a private area. MVS assigns a separate address space to each user to prevent users from violating each others' address space. MVS uses multiple storage protect keys to protect the system and subsystems from unauthorized users. Before MVS performs services on behalf of a user, it takes steps to prevent possible security violations (e.g., the use of invalid control blocks or the execution of unauthorized code) and to avoid user-induced system failures due to improperly specified requests.

Under MVS, the information in real storage is protected from unauthorized use by means of multiple storage protect keys. A non-addressable protect key consists of a control field in storage and is associated with each 2K block of real storage (a 4K block is used in 308X processors). The key in storage contains the protect key of the owner and a fetch protect bit (as well as the reference and change bits maintained by the hardware and used by the software to make paging decisions).

The protect key protects the associated block of storage from unauthorized modification, while the fetch protect bit protects the block from an unauthorized attempt to read or fetch its contents. When a request is made to modify the contents of a real storage location, the key in storage is compared to the storage protection key associated with the request. If the keys match, the request is satisfied, if not, the system rejects the request and issues a program exception interrupt. When a request is made to access (read or fetch) the contents of a real storage location, the request is satisfied unless the block of storage is fetch protected. If the real storage location is fetch protected, the key in storage is compared to the key associated with the request and the resulting action is dependent upon whether or not the keys match.

2.4 SYSTEM INTEGRITY

Requirement:

Hardware and/or software features shall be provided which can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the Trusted Computing Base.

Satisfied By:

Several IBM supplied programs can be used to verify the correct operation of the hardware and the correct format of the RACF data set. The On-Line Test Executive Program (OLTEP) checks for the correct operation of the hardware. The ICHUT200 utility program checks the RACF data set for correct format.

In addition, MVS maintains the SYS1.LOGREC data set for the purpose of error recording. This data set is non-sharable and provides a record of all detected hardware failures and selected software errors and system conditions. Information about each incident is written into SYS1.LOGREC by the system recording routines and can be retrieved by using the environmental recording, editing and printing service aid (IFCEREP1). The IFCEREP1 output can be used for diagnostic and/or measurement purposes to maintain the devices and to support the system control program.

The IFCDIP00 service aid initializes SYS1.LOGREC during system initialization. IFCDIP00 creates a header record and a time stamp record for the SYS1.LOGREC data set and allocates space for the data set which must reside on the system residence volume.

A record is made on SYS1.LOGREC for every detected hardware or software failure and system condition that has an associated recording request or recording routine. The records contain different types of data that document failures and system conditions. The records are stored in chronological order on SYS1.LOGREC. In general, each record contains:

- Relevant system information at the time of the failure.
- Device hardware status at the time of the failure.
- Results of any device/control unit recovery attempt.
- Results of any software system recovery attempt.
- Statistical data.

There are various types of records, containing device- or incident-dependent information that can be recorded on SYS1.LOGREC, which contain complete and specific information for the device, and type of failure or system condition that caused it to be written.

Recording Machine Check records are recorded on SYS1.LOGREC whenever the following detected machine failures occur:

- Central Processing Unit (CPU) processor
- Storage
- Storage Key
- Timer

When a machine failure occurs, the Machine Check Handler (MCH) receives control via a machine-check interrupt for a soft failure (one that was corrected by the hardware retry features) or for a hard failure (one that could not be corrected by the retry features).

If the machine check interrupt is for a soft failure, the MCH uses the environmental and model independent information describing the failure to build an MCH record. After formatting the information, the MCH passes control to the Recovery Termination Manager (RTM). The RTM then invokes the recording request routine which queues the MCH record on the asynchronous

output queue and posts the asynchronous recording task. The recording task asynchronously scans the output queue and issues an appropriate Supervisor Call (SVC) to write any records on this queue to SYS1.LOGREC.

If the machine check interrupt is for a hard failure, the MCH analyzes the information in the model independent logout area, isolates the error, and provides a record of the analysis to the RTM. The RTM then takes the same actions as it does for a soft failure.

With each Initial Program Load (IPL) the system begins a sequential count of errors. The sequence number is therefore unique for each detected software error or machine failure. The sequence number remains constant for subsequent software records associated with the same error (although the time stamp may change). Software records are recorded on SYS1.LOGREC for hardware detected hardware errors, hardware detected software errors, operator detected errors and software detected software errors. For error recording purposes, error data is collected in the System Diagnostic Work Area (SDWA) to assist in identifying the System Control Program (SCP) error and then invoke the RTM.

2.5 SECURITY TESTING

Requirement:

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the Trusted Computing Base.

Satisfied By:

Testing results appear throughout this report. The security features of the RACF/MVS system were tested and found to work as claimed in the documentation. No obvious ways to bypass the security mechanisms of RACF were discovered. Additional attempts were made to bypass store or fetch protection, password checking, and other RACF protection features in order to obtain unauthorized access or control. None of these attempts succeeded.

Penetration testing is not required in class C1 of the Criteria. However, various attempts were made to bypass RACF security mechanisms and gain unauthorized access to the RACF data set. These attempts were done while logged in as a RACF defined user and all attempts were unsuccessful.

It should be noted that, as RACF was originally targeted at the C2 class, the testing that was performed was intended to be sufficient to pass the C2 requirements and followed the guidelines for a C division system.

2.6 DOCUMENTATION

Four types of documentation are required:

2.6.1 SECURITY FEATURES USER'S GUIDE

Requirement:

A single summary, chapter or manual in user documentation shall describe the protection mechanisms provided by the Trusted Computing Base, guidelines on their use, and how they interact with one another.

The following document satisfies this requirement:

1. OS/VS2 MVS Resource Access Control Facility (RACF): General Information Manual, SC28-0722-6 which contains overview information including definitions of RACF terms and a description of RACF functions.

   a. Chapter 2 (pages 17-30) describes the protection mechanisms of RACF.

   b. Chapter 3 (pages 31-35) provides guidelines on the use of the security features of RACF.

   c. Chapter 2 (pages 17-30)
   Chapter 4 (pages 35-40) describe how the protection mechanisms of RACF interact with one another.

2.6.2 TRUSTED FACILITY MANUAL

Requirement:

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility.

The following document satisfies this requirement:

1. OS/VS2 MVS Resource Access Control Facility (RACF): Installation Reference Manual, SC28-0734-4.

   a. Chapter 3 (page 3-31) and Chapter 6 (pages 6-1 - 6-13) present cautions about privileges that should be controlled.

2.6.3 TEST DOCUMENTATION

Requirement:

The system developer shall provide to the evaluators a document that describes the test plan and results of the security mechanisms' functional testing.

1. This requirement is satisfied by documentation that the evaluation team reviewed at the IBM facility at Wappinger Falls, NY.

2.6.4 DESIGN DOCUMENTATION

Requirement:

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the Trusted Computing Base. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

The following documents satisfy this requirement:

1. OS/VS2 MVS Resource Access Control Facility (RACF): General Information Manual, SC28-0722-6 which contains overview information including definitions of RACF terms and a description of RACF functions.

   a. Introduction (pages 1-15) provides a description of IBM's philosophy of protection and an explanation of how this is translated into the TCB.

2. OS/VS2 MVS Resource Access Control Facility (RACF): Installation Reference Manual, SC28-0734-4.

   a. Chapter 2 (pages 17-30)
   Chapter 4 (pages 35-40) describe how the protection mechanisms of RACF interact with one another.

SECTION 3

DEFICIENCIES AGAINST CLASS C2 REQUIREMENTS

RACF MEETS ALL OF THE REQUIREMENTS OF CLASS C2 EXCEPT FOR THAT INCLUDED IN THIS SECTION. THIS DEFICIENCY IS THE REASON WHY RACF WAS NOT GIVEN A HIGHER RATING.

3.1 OBJECT REUSE

Requirement:

When a storage object is initially assigned, allocated, or reallocated to a subject from the TCB's pool of unused storage objects, the TCB shall assure that the object contains no data for which the subject is not authorized.

Evaluation Results:

Although each page of main memory is zeroed upon allocation, it is possible to access residue in secondary storage (e.g., disk).

An Access Method Service (IDCAMS), which is supplied as a part of MVS, does provide the ability to specify erasing during the deletion of secondary storage for VSAM data sets. This can be accomplished in two ways: first, the user can specify the ERASE parameter at data set creation when using the DEFINE command; secondly, the user can specify the ERASE parameter of the DELETE command during deletion.

Although the capability exists to erase data, these methods are not sufficient to satisfy the requirement of the Criteria for the following two reasons:

1. Storage is not erased when a non-VSAM data set is deleted or when the system releases the temporary work files and data sets that it uses. This makes it possible to scavenge residue from deleted data sets.

2. The decision to erase the data from the data set is left to the discretion of each individual user. This decision should be made by the installation and should automatically be done under the control of the Trusted Computing Base.

During the testing, the following intelligible data residues were obtained: JCL from a previous job, a deleted file created by the team, FORTRAN source code, and a part of another data file. Therefore, although there exists the capability to control data residue in VSAM data sets, the fact that this control is

left up to the individual user and that non-VSAM and temporary data sets cannot be controlled results in the class C2 requirement not being satisfied.

It should be noted, however, that it appears that this problem can be corrected. There exists a documented set of modifications for MVS Release 3.8 that cause all disk space to be erased before becoming eligible for reuse [2]. These modifications, however, were not present in the system used for the functional testing of this evaluation. [The reader of this report should realize that these modifications are not supported by IBM and, therefore, can not be considered as a part of this evaluation.]

SECTION 4

THOSE REQUIREMENTS WHERE RACF EXCEEDS CLASS C1

THIS SECTION ADDRESSES ONLY THOSE REQUIREMENTS THAT RACF SATISFIES ABOVE CLASS C1.

4.1 AUDIT (CLASS C2)

Requirement:

The Trusted Computing Base shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators or system administrators and/or system security officers. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity.

Satisfied By:

RACF generates records for detected unauthorized attempts to enter the system, authorized accesses and/or detected unauthorized attempts to access RACF protected resources, and authorized and/or detected unauthorized attempts to modify information about RACF users, groups of users, or RACF protected resources. RACF writes audit records to the MVS System Management Facility (SMF) data sets (SYS1.MAN*) and sends messages to the system and/or optional security console (any console defined with a message route code of 9) regarding access attempts. The audit data can and should be protected by RACF (the protection of the audit data is a requirement for this class, therefore, whether or not this requirement is met is dependent upon the installation's defining the audit data sets to RACF).

During the testing, selective auditing was implemented for specified authorized accesses, for unauthorized access attempts by specified users, and for specified resources. A series of authorized and unauthorized accesses were attempted, manually logged, and found to match the audit reports generated by the RACF Report Writer.

RACF provides options for the selection of varying levels of auditing. Privileged RACF TSO commands are provided to list the contents of RACF profiles. The RACF Report Writer selects SMF records produced by RACF and prepares reports. Reports can be requested which provide these records in selectable formats that describe:

- Attempts to access a particular RACF-protected resource in terms of user identity, number and type of successful accesses, and number and type of security violations.

- User and group activity.

- Summaries of system and resource use.

During the testing, attempts were made to obtain unauthorized access to audit files and to circumvent auditing. All of these efforts, including an attempt to gain unaudited access to objects through illegal exploitation of the Global Access Checking Facility, were unsuccessful.

4.2 DOCUMENTATION (CLASS C2)

4.2.1 TRUSTED FACILITY MANUAL

Additional Requirement:

In addition to the class C1 requirements, the procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given.

The following document satisfies this requirement:

1. OS/VS2 MVS Resource Access Control Facility (RACF): Installation Reference Manual, SC28-0734.

   a. Chapter 13 (pages 13-17 - 13-51) presents the detailed audit record structure for each type of audit report.

4.3 IDENTIFICATION AND AUTHENTICATION (CLASS C2) (NO ADDITIONAL REQUIREMENTS ABOVE CLASS C2)

Additional Requirement:

The Trusted Computing Base (TCB) shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

Satisfied By:

RACF requires that each user attempting to access any RACF protected resource in the system be defined to RACF through a unique userid. If a user is not defined to RACF, all his access attempts (except when universal access (UACC) has been specified as some value other than NONE) to RACF protected resources are denied.

During the testing, various access attempts were manually logged and found to match the results returned by the RACF Report Writer.

4.4 DISCRETIONARY ACCESS CONTROL (CLASS B3)[1]

Requirement:

The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., access control lists) shall allow users to specify and control sharing of those objects. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of specifying, for each named object, a list of named individuals and a list of groups of named individuals with their respective modes of access to that object. Furthermore, for each such named object, it shall be possible to specify a list of named individuals and a list of groups of named individuals for which no access to the object is to be given. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

Satisfied By:

Although RACF normally protects only those resources that are defined to it, RACF can provide protection by default. A

1. Although RACF satisfies this feature at the B3 level, RACF does not satisfy any of the assurance requirements above the C2 level.

"default" access rule capability is available with profile modeling. Profile modeling can be used to implement "default" protection by defining a model profile for each user and/or group. This model profile can contain the universal access authority, auditing flags, owner, level, installation-defined data, and access lists. Testing verified that model profiles can be created on a user or group basis to contain the default access parameters for the newly created data set. Further, the RACF SETROPTS command can be used to turn on RACF resource checking for resource classes defined to RACF, so that all accesses to that resource are checked by RACF.

Other defaults are supplied with individual RACF commands, e.g., the AUDIT option for a DASD data set defaults to the audit of access failures. Further, installation exits can be programmed for an always-call situation in which different implementations can be tailored for the exact needs of the installation.

The ability to exclude access to a data set down to the granularity of a single user is available in the RACF/MVS system. Entries can be made to the RACF profile data set that can specify a specific user and assign that user an access authority of NONE. These entries can be made by the owner of the resource or by a security administrator (a user with the SPECIAL attribute).

SECTION 5

EVALUATORS' COMMENTS

The object reuse requirement of class C2 requires that all storage objects be clear of data for which the user is not authorized before that object is given to the user. While RACF/MVS does clear pages upon allocation for main memory, it is possible to obtain residue from secondary storage devices.

There are, however, methods through which an installation may decrease the severity of the problem. First, MVS does provide the ability to clear storage upon deletion for VSAM data sets through the use of the DELETE command with the ERASE parameter. Also, the user can specify erase on delete through the use of the ERASE parameter of the DEFINE command at object creation time (or at some later time). If these methods are always used, residue will not exist after the deletion of VSAM data sets. However, residue will still exist in non-VSAM and temporary data sets created either by the user or by the system in its normal operation. Therefore, these methods will not satisfy the Criteria. The erasing of data must be done for all objects in the system and it must be done automatically and under the control of the Trusted Computing Base (i.e., it can not be left to the discretion of each individual user).

Also, for particularly sensitive information, RACF can be used to restrict and/or allow access to a physical storage device to an authorized individual or group of mutually unsuspicious users. This method would not prevent the ability to scavenge residue but the user performing the scavenging may have had legal access to the data when it was resident in an active storage object. Therefore, the user may not be gaining access to data that he should not otherwise have. This does <u>not</u> mean that residue scavenging can be prevented, only that it <u>may</u> be possible to reduce, not eliminate, the risk and damage that scavenging may cause.

There also exists a set of modifications for the MVS Release 3.8 operating system that cause all disk space to be erased before becoming eligible for reuse. This report is available through the National Technical Information Service (NTIS, report number ADA091957).

The audit capabilities of RACF/MVS are versatile and extensive. With the exception of the monitoring of covert channels and auditing based on object security level, RACF/MVS satisfies the other audit requirements of the Criteria. RACF does not satisfy the class B1 audit requirement of the Criteria because the system does not support security levels. To audit by security level pre-supposes that the system supports security

levels as they are defined in the Criteria.

In the RACF/MVS system, there exists a LEVEL field that is associated with all RACF defined data sets that is recorded in all audit record entries and can be used as a selection parameter when generating audit reports. This field, however, is not treated as a security level as defined in the Criteria. If the system did support security levels, it appears that this field may be sufficient to satisfy the class B1 audit requirement if the installation audited all accesses to all objects in the system and the audit utilities were used to generate reports by selected LEVEL field values.

RACF/MVS also possesses extensive back-up and recovery facilities for the RACF data set. These facilities, however, do not satisfy the Trusted Recovery requirement of the Criteria because the requirement of the Criteria is that a secure initial state must be attainable and it must be shown that it is possible to recover to this state without a protection compromise after a system failure.

For the maximum security possible, RACF should be implemented to supply default protection of all resources in the system, all users of the system should be defined to RACF and given the minimum amount of authority that will allow them to efficiently and effectively use the system. Passwords should be enforced and regular password change should be implemented. Finally, the RACF audit facilities should be used to the maximum, reasonable extent and the RACF Report Writer should be used regularly to obtain information on which users are utilizing what resources and how.

SECTION 6

CONCLUSIONS

The DoDCSC evaluation team has determined that the highest class at which RACF/MVS satisfies all the specified requirements of the Criteria is class C1 and therefore RACF/MVS has been assigned a class C1 rating.

Further, RACF/MVS was found to meet or exceed all requirements of class C2 except for the Object Reuse requirement.

RACF/MVS, as delivered by IBM, does not recognize security classification levels or category compartments and cannot be used to provide mandatory access control.

Finally, RACF's strong discretionary access controls and audit features provide significant improvements to the security of the MVS operating system.

REFERENCES

1. Department of Defense Trusted Computer System Evaluation Criteria, Ft. Meade, MD: DoD Computer Security Center, 15 August 1983.

2. Gwatking, J.C., Automatic Erasure of Released Disk Space on an IBM 370 Computer Using the MVS Operating System, NTIS # AD-A091957, Department of Defence, Defence Research Centre, Salisbury, South Australia, June 1980.

RACF Publications:

3. OS/VS2 MVS Resource Access Control Facility (RACF): General Information Manual, SC28-0722-6.

4. OS/VS2 MVS Resource Access Control Facility (RACF): Command Language Reference, SC28-0733-3.

5. OS/VS2 MVS RACF General User Command Reference Card, SX28-0609-1.

6. OS/VS2 MVS Resource Access Control Facility (RACF): Installation Reference Manual, SC28-0734-4.

7. OS/VS2 MVS Resource Access Control Facility (RACF): Messages and Codes, SC38-1014-3.

8. OS/VS2 MVS Resource Access Control Facility (RACF): Program Logic Manual, LY28-0730-2.

OS/VS System Publications:

9. OS/VS2 JCL, GC28-0692.

10. OS/VS2 System Programming Library: Supervisor, GC28-0146-0.

11. OS/VS2 Supervisor Services and Macro Instructions, GC28-0683.

12. OS/VS2 System Programming Library: Job Management, GC28-0627.

13. OS/VS2 System Programming Library: System Management Facilities (SMF), GC28-1030.

14. OS/VS2 System Programming Library: Initialization and Tuning Guide, GC28-1029.

15. OS/VS2 System Programming Library: TSO, GC28-0629.

16. OS/VS2 TSO Command Language Reference, GC28-0646-4.

17. OS/VS2 TSO Terminal User's Guide, GC28-0645-4.

18. Operator's Library: OS/VS2 MVS System Commands, GC28-1031.

19. OS/VS2 Access Method Services, GC26-3841.

20. OS/VS Virtual Storage Access Method (VSAM) Programmer's Guide, GC26-3838.

21. OS/VS2 System Programming Library: Data Management, GC26-3830.

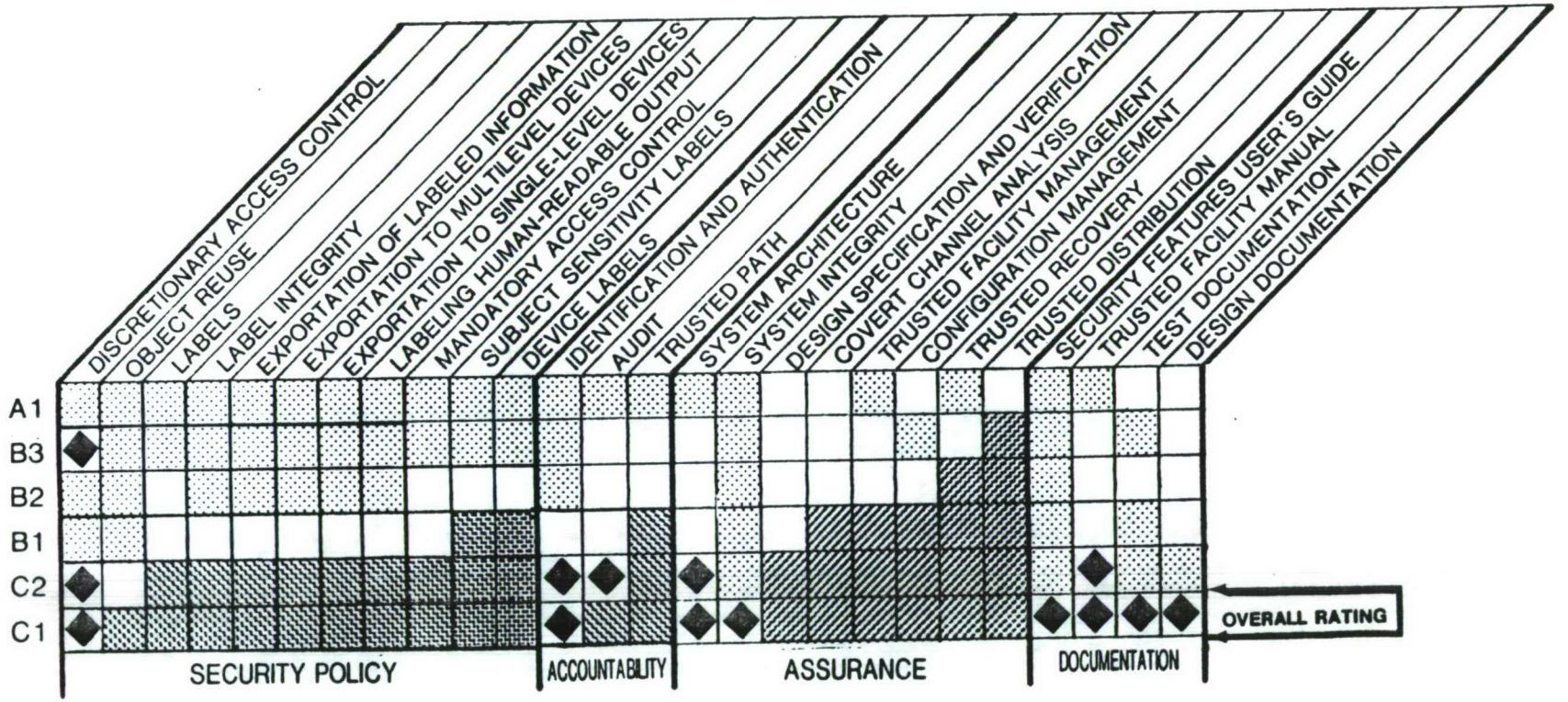
22. OS/VS2 MVS Data Management Services Guide, GC26-3875.

GLOSSARY

This glossary contains the abbreviations contained in this report along with their expanded meanings and page of first mention.

ADP	Automatic Data Processing, 5
ADSP	Automatic Data Set Protection, 3
CICS	Customer Information Control System, 7
CPU	Central Processing Unit, 10
Criteria	Department of Defense Trusted Computer System Evaluation Criteria, iv
DASD	Direct Access Storage Device, 3
DoDCSC	Department of Defense Computer Security Center, iv
EPL	Evaluated Products List, 1
GAC	Global Access Checking, 6
IBM	International Business Machines, Corp., iv
IDCAMS	an Access Method Service, 14
IMS	Information Management System, 7
IPL	Initial Program Load, 11
ISPF	Interactive System Productivity Facility, 2
JCL	Job Control Language, 8
JES2	Job Entry Subsystem 2, 2
JES3	Job Entry Subsystem 3, 8
MCH	Machine Check Handler, 10
MVS/SP	Multiple Virtual Storage/System Product, iv
NCCF	Network Communication Control Facility, 7
NTIS	National Technical Information Service, 20
OLTEP	On-Line Test Executive Program, 9

TRUSTED COMPUTER SYSTEM EVALUATION SUMMARY CHART



NO REQUIREMENTS FOR THIS CLASS

NO ADDITIONAL REQUIREMENTS FOR THIS CLASS

MEETS OR EXCEEDS THE REQUIREMENTS FOR THIS CLASS

SYSTEM NAME:	Resource Access Control Facility (RACF)
VENDOR:	IBM Corp.
EVALUATION DATE:	23 July 1984

APPENDIX

EVALUATION SUMMARY OF RACF VS. CRITERIA REQUIREMENTS

1.1 DISCRETIONARY ACCESS CONTROL EVALUATION SUMMARY

As a user with the SPECIAL attribute, create a number of user groups with multiple users in each group. Each group should have a member possessing the JOIN and/or CONNECT attribute. Via these users, develop an access control matrix defining users vs. resources with authorized access rights, user groups, and resource groups, and implement via proper entries to RACF profile models.

user	group	user attribute		group authority
user1	G1	GRPACC		CREATE,USE
user2	G1,G3	SPECIAL,ADSP	(1)	JOIN,CONNECT,CREATE,USE
			(3)	CREATE,USE
user3	G2	AUDITOR		CONNECT,CREATE,USE
user4	G1	ADSP		CREATE,USE
user5	G2	SPECIAL,ADSP		JOIN,CONNECT,USE
user6	G2,G3		(2)	USE
			(3)	USE
user7	G3	SPECIAL		JOIN,CONNECT,CREATE,USE
user11	G3	GRPACC,ADSP		CREATE,USE
user12	G3,G4	AUDITOR,GRPACC	(3)	CREATE,USE
			(4)	JOIN,CONNECT,CREATE,USE
user13	G4			USE
user14	G3			USE
user15	G4	GRPACC,ADSP		CREATE,USE
user16	G4			USE
user17	G1			USE
user18	G1,G4	ADSP	(1)	CREATE,USE
			(4)	USE

** ISSUE THE FOLLOWING COMMANDS TO CREATE USERS, USER GROUPS AND TO ASSIGN USER ATTRIBUTES AND PRIVILEGES

```
/  AG (G1,G2,G3,G4)

/  AU user1 PASSWORD(userp1) DFLTGRP(G1)
   AUTHORITY(CREATE,USE) GRPACC

/  AU user2 PASSWORD(userp2) DFLTGRP(G1)
   AUTHORITY(JOIN,CONNECT,CREATE,USE) ADSP SPECIAL
/  CONNECT user2 GROUP(G3) AUTHORITY(CREATE,USE) ADSP
   SPECIAL

/  AU user3 PASSWORD(userp3) DFLTGRP(G2)
   AUTHORITY(CONNECT,CREATE,USE) AUDITOR
```

```
/  AU user4 PASSWORD(userp4) DFLTGRP(G1)
   AUTHORITY(CREATE,USE) ADSP

/  AU user5 PASSWORD(userp5) DFLTGRP(G2)
   AUTHORITY(JOIN,CONNECT,USE) ADSP SPECIAL

/  AU user6 PASSWORD(userp6) DFLTGRP(G2) AUTHORITY(USE)
/  CONNECT user6 GROUP(G3) AUTHORITY(USE)

/  AU user7 PASSWORD(userp7) DFLTGRP(G3)
   AUTHORITY(JOIN,CONNECT,CREATE,USE) SPECIAL

/  AU user11 PASSWORD(userp11) DFLTGRP(G3)
   AUTHORITY(CREATE,USE) GRPACC ADSP

/  AU user12 PASSWORD(userp12) DFLTGRP(G3)
   AUTHORITY(CREATE,USE) GRPACC AUDITOR
/  CONNECT user12 GROUP(G4) AUTHORITY(CONNECT,CREATE,USE)
   GRPACC

/  AU user13 PASSWORD(userp13) DFLTGRP(G4) AUTHORITY(USE)

/  AU user14 PASSWORD(userp14) DFLTGRP(G3) AUTHORITY(USE)

/  AU user15 PASSWORD(userp15) DFLTGRP(G4)
   AUTHORITY(CREATE,USE) GRPACC ADSP

/  AU user16 PASSWORD(userp16) DFLTGRP(G4) AUTHORITY(USE)

/  AU user17 PASSWORD(userp17) DFLTGRP(G1) AUTHORITY(USE)

/  AU user18 PASSWORD(userp18) DFLTGRP(G1)
   AUTHORITY(CREATE,USE) ADSP
/  CONNECT user18 GROUP(G4) AUTHORITY(USE) ADSP
```

****

USING THE RDEFINE AND PERMIT COMMANDS
WRITE SOME ACCESS RULES FOR SYSTEM RESOURCES

****

Attempt to implement various levels of default protection for selected resources, so that they are always under RACF protection.

```
/  *** use the AD command to protect some existing data sets
       and use the AUDIT(ALL) parameter to specify auditing
       of all accesses to these data sets
```

With the ADSP attribute specified, insure that for specified users, newly created objects are protected to the specified default level (create a data set and without writing any access rules, have other users try to access that data set).

*** Log in as user2 and, using ISPF, create a data set named testl.data

*** Log in as users 3,5,6 and try to access that data set through both the read and edit methods:

/ edit testl data old

/ ***write a program that will try to read from testl.data

* Using the users defined in this section, create some data sets. Write some access rules for those data sets and insure that the access rules are enforced.

Attempt to illegally exploit the Global Access Checking Facility to bypass RACF protection.

*** Log in as users 3,5,6 and try to issue the following commands (they should be denied by RACF):

/ RDEFINE GLOBAL DATASET ADDMEM('SYS1.*'/READ)

/ RALT GLOBAL DATASET ADD( )

Write access and resource rules to implement access control down to the granularity of a single user and insure that the specified user may/may not access the specified resource, depending upon the access rule.

Utilizing a selected subset of the system resources, set up generic profiles for a class which should provide default protection for that class's resources (e.g., data sets) whenever the resource name matches an existing generic profile name. Create new data sets and attempt to access them while logged in as different, unauthorized users. Verify that these resources received protection by default.

After logging in as a user with the ADSP attribute, create new data sets as in the above procedure. Login as users not authorized to access these data sets and verify that these data sets are also protected by default.

Login as a user without the SPECIAL attribute and attempt to add a new resource to the Global Access Checking Table by using the RDEFINE command and verify that this is not allowed. Also, while logged on as this same user, attempt to write to this table with the RALTER command (assuming that this user does not own the resource that he is trying to alter in the table). Verify that this is not allowed. Repeat this procedure for different users with different attributes. Attempt to modify the table by changing the file either through an editor or by attempting to replace it with a different table. Verify that a user not

possessing the SPECIAL or AUDITOR attributes cannot enable or disable the GAC facility by executing the SETROPTS command with the appropriate parameters.

Verify that individual accountability is enforced (i.e., insure that a users actions are always logged as being performed by that user). Keep a manual log and check the users actions in the log against the reports produced by the Report Writer.

1.2 OBJECT REUSE EVALUATION SUMMARY

Using JCL, allocate disk space and attempt to print its contents. In order to verify that another user's residue can be obtained, create a very large file of recognizable information. Expand that file until it fills the entire disk space of the owner. Next delete the file, and log on as a different user in a different group who did not have access to the deleted data set. This new user shall not possess any special attributes that would enable him to bypass RACF/MVS protection. Execute the scavenging JCL and check to see if there are pieces from the previously deleted data set.

1.3 IDENTIFICATION AND AUTHENTICATION EVALUATION SUMMARY

Insure the provision of password support for password syntax, expiration dates, and required password change by defining six users to RACF and assigning their passwords using six different password configurations. (No syntax rule defined to RACF at this time).

```
/  AU user21 PASSWORD(ulgrep)
/  AU user22 PASSWORD(2Petyr3) SPECIAL
/  AU user23 PASSWORD(PS45hr22) AUDITOR
/  AU user24 PASSWORD(3*gr%P)
/  AU user25 PASSWORD(upasswd5) SPECIAL ADSP
/  AU user26 PASSWORD(wLOGON6) ADSP
```

Define a password syntax rule to RACF and observe what actions RACF takes, if any, to force these users to change their passwords so that they comply with the syntax rule.

```
/  SETROPTS PASSWORD(RULE1(LENGTH(5)ALPHA(1:5))
                     RULE2(LENGTH(6:8)ALPHANUM(1:8)))
```

Define a new user to RACF and insure that his password must comply with the syntax rule.

```
/  AU user27 PASSWORD(user27urj) SPECIAL
```

*** This password is illegal, what does RACF do in this case.

For one of these users, set the password change interval so that his password will expire. After the interval passes, insure that RACF forces the user to change his password before being allowed access to the system.

```
/  PASSWORD USER(user21) INTERVAL(1)
```

Attempt to gain access to the system or to the RACF data sets to obtain passwords by illegally using the ADDUSER, ALTUSER, PERMIT and/or any other commands.

```
/  PE 'RACF data set name' USER(user21) ACCESS(READ)
/  AU user28 PASSWORD(userp28) SPECIAL AUDITOR
/  ALU user25 SPECIAL AUDITOR
```

*** THE ABOVE COMMANDS ARE TO BE ENTERED BY BOTH A USER WITH NO PRIVILEGES AND A USER WITH THE AUDITOR PRIVILEGE

Set the limit on the number of incorrect logon attempts at three. Exceed this limit using a legal userid but an incorrect password and insure that the userid is suspended until it is reset by the system security administrator. A message concerning these illegal logon attempts should be sent to the system security and/or operator console.

```
/  SETROPTS PASSWORD REVOKE(3)
```

Attempt to create a duplicate user id (an id that is not unique), what does RACF do in this situation?

```
/  AU user21 PASSWORD(hryuf3)
```

Attempt to create a user with a non-unique password, will RACF allow this?

```
/  AU user30 PASSWORD(ulgrep)
```

1.4 AUDIT EVALUATION SUMMARY

Attempt different accesses, both authorized and unauthorized, by different users, groups, etc. Manually log these access attempts and use the RACF Report Writer to examine the SMF records to insure that all accesses and attempts have been properly accounted and recorded.

Attempt to obtain illegal access to the audit files. Attempt to circumvent auditing for a specified access attempt by first overloading audit files by appending data to the audit files and/or by creating a series of illegal access attempts prior to the specified access.

Specify monitoring and console notification for various occurrences and accumulations of events. Insure that each occurrence or accumulation of events invokes the transmission of the appropriate message to the operator and/or security administrator.

Specify the console(s) to which the security violation messages are to be written. Insure that the appropriate messages are transmitted to the console(s) on the occurrence of the maximum number of violation attempts.

```
/ DISPLAY CONSOLES
```

* This command will display console information. If a different console id desired as the security console, use the VARY command to change the console designation.

Login as different users possessing different attributes, and attempt to read, write, or delete the auditing data base.

Attempt to gain access to object while bypassing the auditing system (e.g., exploit the GAC facility to bypass auditing).

In performing the above, keep a manual log of every action performed. Finally, invoke the RACF Report Writer and compare its output to the manual log.

*** This should be implemented by a RACF defined AUDITOR.

```
/  RACFRW GENSUM
/  LIST
/  SUM GROUP
/  SUM GROUP BY(RESOURCE)
/  SUM USER
/  SUM USER BY(RESOURCE)
/  SUM EVENT
/  SUM EVENT BY(RESOURCE)
/  SUM RESOURCE
/  SUM RESOURCE BY(GROUP)
/  SUM RESOURCE BY(USER)
/  SUM RESOURCE BY(EVENT)
/  SUM COMMAND
/  SUM COMMAND BY(GROUP)
/  SUM COMMAND BY(USER)
/  SUM COMMAND BY(EVENT)
/  END
```

*** Using a userid without the AUDITOR privilege, attempt to invoke the RACF report writer.

```
/  * USE THE ABOVE COMMANDS AND user6 TO ATTEMPT THIS TASK.
```

Insure that the RACF Report Writer includes, for each entry, the userid, resource(s), type of access attempted or obtained and the time of access. Also, insure that the user's actions are always logged as being done by that user.

/ Compare the machine generated reports to the manual log.

1.5 RESOURCE ENCAPSULATION EVALUATION SUMMARY

Attempt to obtain various accesses to RACF protected resources. Insure that only legal accesses are allowed, that all other access attempts are prohibited and appropriately logged in the SMF records, and that complete, properly formatted reports are available via the RACF Report Writer.

1.6 SYSTEM ARCHITECTURE EVALUATION SUMMARY

Insure that system level data structures, both MVS and RACF, are afforded protection against unauthorized modification.

*** The test for this requirement is included in sections 1.1 and 1.3 of this test plan.

1.7 SYSTEM INTEGRITY EVALUATION SUMMARY

Verify by inspection that IBM-supplied MVS and RACF utility programs provide sufficient assurance of correct operation.

The Criteria does not require the validation of software at the class C2 level, therefore, the MVS utility programs which check for the correct operation of the hardware may satisfy the requirement.

1.8 SECURITY TESTING EVALUATION SUMMARY

Using the system documentation, determine which security features and/or class C2 requirements have not already been included in the test plan and develop tests to insure that these features work as claimed.

Make additional attempts to bypass store or fetch protection, password checking, and other RACF protection features in order to obtain unauthorized access or control.

Inspect audit files to insure that the above actions have been logged according to the audit requirements specified for the encapsulated resources.

1.9 DOCUMENTATION EVALUATION SUMMARY

For the class C2 documentation requirements (items 1.9.1-1.9.4 below), examine the RACF documentation that appears below each requirement to determine if the requirement is satisfied by the documentation.

1.9.1 Security Features Users Guide:

* OS/VS2 MVS Resource Access Control Facility (RACF): General Information Manual, GC28-0722.

1.9.2 Trusted Facility Manual:

* OS/VS2 MVS Resource Access Control Facility (RACF): Installation Reference Manual, SC28-0734-4.

1.9.3 Test Documentation:

* This requirement is satisfied by documentation that the evaluation team reviewed at the IBM facility in Wappinger Falls, NY.

1.9.4 Design Documentation:

* OS/VS2 MVS Resource Access Control Facility (RACF): General Information Manual, GC28-0722.

* OS/VS2 MVS Resource Access Control Facility (RACF): Installation Reference Manual, SC28-0734-4.